


IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF RHODE ISLAND

IN THE MATTER OF THE SEARCH OF  
TARGET DEVICES

Case No. 1:18 MJ 306 PAS  


**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Brandon Henderson, being duly sworn, hereby depose and state the following:

**A. Agent Background**

1. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am an officer of the United States empowered by law to conduct criminal investigations and make arrests. I have been a law enforcement officer for over 13 years. I am employed by the United States Secret Service. In my capacity as a Special Agent with the United States Secret Service, I investigate a variety of offenses and violations of federal criminal law, including offenses involving bank fraud, wire fraud and identity theft.

2. Prior to my assignment with the United States Secret Service, I was a Sergeant Detective with the Opelika Police Department, located in Opelika, AL, for nine and a half years. I am a graduate of the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynn County, Georgia, and the Special Agent Training Program at the James J. Rowley Training Center at Laurel, Maryland. Through these programs, I received specialized training in investigating various federal crimes including, but not limited to, manufacturing of

counterfeit access devices and the use of fraudulent identifications and credit cards, bank fraud, wire fraud, and identity theft. In my capacity as a Secret Service Special Agent, I have conducted or participated in investigations involving the manufacture, trafficking or use of counterfeit credit cards and identification cards, as well as bank fraud, wire fraud, and identity theft.

**B. Warrant Requested**

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

3. The property to be searched is:

- a. Motorola Moto phone (Gold in color) – IMEI – 355674083917180
- b. Toshiba USB flashdrive (white in color) – S/N – 134013XA475CARGO1S
- c. Samsung phone (grey in color, model SM-J327T1) – IMEI – 354256/09/752960/6
- d. Coolpad phone (black in color) – IMEI – 862429030253312
- e. LG phone (grey in color, model LM-X210MA) – IMEI – 356233-09-257593-2
- f. 16GB SanDisk SD Card - BL1418250167G
- g. 16GB SanDisk SD Card – BL1731250835G
- h. LG (grey in color, model LM-X210MA) – IMEI – 356233-09-258022-1
- i. Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091035663
- j. Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091522652
- k. iPhone X (silver in color) a label with the #13 has been affixed to the phone
- l. iPhone X (space grey in color) a label with the #14 has been affixed to the phone
- m. LG phone (black in color, model LM-X210MA) – IMEI – 357093-09-047884-7
- n. LG phone (grey in color, model LM-X210MA) – IMEI – 356233-09-664656-4
- o. 64GB SD card in Canon SanDisk – BN1734951494G
- p. Apple Macbook Pro 15” (MODEL A1707) S/N – C02VW0DYHTD6
- q. Apple iMac 27” – S/N – C02VW37VHX87

(hereinafter TARGET DEVICES) Currently stored at the U.S. Secret Service evidence locker, Providence, Rhode Island.

The applied-for warrant would authorize the forensic examination of the TARGET DEVICES for the purpose of identifying electronically stored data particularly described in Attachment A.

4. I submit this affidavit in support of an application for a warrant under Rule 41 of the Federal Rules of Criminal Procedure to search and electronically stored evidence located on the TARGET DEVICES.

5. I have probable cause to believe that the TARGET DEVICES contain evidence of federal crimes including, Conspiracy to commit Aggravated Identity Theft, 18 U.S.C. § 1029(b)(2); Identity Theft, 18 U.S.C. § 1028A, Access Device Fraud, 18 U.S.C. § 1029, Bank Fraud 18 U.S.C. § 1344 and Fraudulent Use of Social Security Numbers 42 U.S.C. § 408(a)(7)(B).

6. This investigation is being conducted jointly with agents of the United States Secret Service, United States Social Security Administration, Office of Inspector General, and the United States Postal Inspection Service. In addition to the participation of the “lead agencies”, I am aware that law enforcement officers from numerous police departments have investigated various incidents and have filed official reports documenting their findings. Because of my personal participation in the investigation, review of reports submitted by other law enforcement personnel, and my consultations with other law enforcement officers, I am familiar with this investigation.

**TECHNICAL TERMS**

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets

typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

- c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training, experience, and research, I know that the TARGET DEVICES have capabilities that allow them to store electronic data including photographs, screenshots, SMS text messages, emails, social media instant messaging and a variety of electronic data used to perpetrate identity theft, wire fraud, bank fraud and conspiracy. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

#### **ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

9. Based on my knowledge, training, and experience, I know that the TARGET DEVICES can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

10. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

11. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

**PROBABLE CAUSE TO BELIEVE THAT FEDERAL CRIMES WERE COMMITTED**

12. The investigation establishing the probable cause to search the TARGET



DEVICES is the result of a collaborative effort on the part of the United States Secret Service, the United States Social Security Administration Office of Inspector General Criminal Investigations and the United States Postal Inspection Service.

13. The federal investigation began on April 19, 2017, when I received reports relating to possible violations of federal law including access device fraud and aggravated identity theft. This initial investigation resulted in the issuance of an arrest warrant for Reynaldo Martinez (DOB: 08/06/XXXX) as well as a search warrant for his Roosevelt Avenue Central Falls, Rhode Island apartment. On May 24, 2018, the U.S. Secret Service arrested Martinez and executed the federal search warrant for his apartment. Furniture and electronics purchased through identity fraud were located in Rodriguez's apartment and agents seized the items as evidence.

14. Reynaldo Martinez was returned to the Secret Service office in Providence, Rhode Island. He was provided his *Miranda* warnings and agreed to participate in an interview. He signed a written *Miranda* form and agreed to answer questions. The interview was video and audio recorded. During the interview, Reynaldo Martinez admitted to engaging in identity theft. He explained how he obtained the personal information of his victims and how he worked with others to secure fraudulent driver's licenses. He stated that he would memorize the victim's information. He stated he used a rap song to incorporate the individualized information to aid him in the memorization process. I asked Martinez about the male who was in his apartment with him, Jason McDonald. Martinez reported that McDonald is his uncle. He told me that his uncle does not like what he (Martinez) does. I confronted Martinez with the fact that his uncle was in possession of a false identification. He then stated "he does what he does." Martinez denied having obtained any false identifications for his uncle. He stated that he does not know what his uncle does but "to be honest even if I knew I would not tell you."

15. During this interview, Martinez advised me that he had been obtaining counterfeit driver's licenses from an individual who he identified as "Mono." Martinez advised me that Mono maintains computer equipment and a specialized printer used to create identifications. Martinez told me that he had personally obtained identifications from "Mono" and that Mono has access to holograms used by state governments as authentication features on driver's licenses. Martinez described where Mono lived and actually pointed out the building. The address described by Martinez is 413 Central Avenue, Pawtucket, Rhode Island, the American Wire building. Brady-Sullivan property management manages this converted factory building. A grand jury subpoena was served upon Brady-Sullivan for leasing records related to the apartment described by Martinez as well as a second apartment linked by Brady-Sullivan to the identified apartment. Records obtained from Brady-Sullivan, including color copies of identification documents provided by the tenants, showed that "Mono" is actually Octavio Andres Difo-Castro. Difo-Castro has been identified by seven separate witnesses as being a very active identity thief. No less than two witnesses have provided sworn grand jury testimony that Difo-Castro recruits people to use fraudulent identities to obtain various items including cellular telephones, electronics, furniture and building supplies. These witnesses have further testified that Difo-Castro creates counterfeit identifications and maintains computers and printers for purpose of doing so.

16. Incident to the May 24, 2017 arrest of Martinez, agents seized an Apple iPhone that Martinez admitted belonged to him. During the interview process, Reynaldo Martinez provided the password to access the iPhone seized. I contacted cellular telephone analyst, Detective Theodore Michaels, of the Providence Police Department and requested his assistance in analyzing Martinez's cell phone. Detective Michaels is a court-recognized expert in the field

of cellular telephone analysis. He agreed to access and copy Martinez's iPhone as well as create readily searchable reports to better facilitate the recognition and collection of electronic evidence. I provided Detective Michaels the iPhone seized from Reynaldo Martinez's apartment. Using standardized practices and procedures, Detective Michaels copied the data from the phone and provided investigators with compact discs containing the electronic evidence.

17. In addition to numerous photographs of Martinez, agents located numerous text messages between Martinez, Donald Wicklund, Jason McDonald and others evidencing the fact that Martinez was exchanging stolen personal identification information with these men. Martinez had also listed a contact telephone number for "El Mono." Your affiant has come to learn that El Mono is a nickname for a former associate of Martinez, Octavio Andres Difo-Castro.

18. Based in part on the text messages located in Martinez's phone, coupled with information developed through witness interviews and the examination of certain documentary and video evidence, investigators concluded that Donald Wicklund and Jason McDonald were involved in identity theft, wire fraud and bank fraud. As a result of that part of the investigation, the following individuals have been indicted and convicted of a variety of federal offenses.

- a. **Reynaldo Martinez** was indicted on June 20, 2017 charged with Conspiracy to Commit Access Device Fraud, 18 U.S.C. §1029(b)(2), Access Device Fraud, 18 U.S.C. §1029(a)(2), Attempted Access Device Fraud 18 U.S.C. § 1029(b)(1) and Aggravated Identity Theft 18 U.S.C. § 1028(A). On August 15, 2017, the grand jury returned a superseding indictment that charged Martinez with additional counts including Bank Fraud 18 U.S.C. § 1344(1) and Interstate Transportation of Stolen Goods 18 U.S.C. § 2314. On November 10, 2017, Martinez plead guilty to the

superseding indictment. U.S. District Court Judge John J. McConnell sentenced Martinez to a total of 48 months incarceration.

- b. **Jason McDonald** was indicted on October 24, 2017, in a four-count indictment that charged Conspiracy to Commit Bank Fraud, 18 U.S.C. §§ 1349 and 1344, Attempted Bank Fraud, 18 U.S.C. §§ 1349 and 1344, Fraudulent Use of a Social Security Number 42 U.S.C. § 408(a)(7)(B) and Aggravated Identity theft 18 U.S.C. § 1028(A). On March 23, 2018, McDonald was charged by way of criminal information with a single count of Conspiracy to Commit Wire Fraud, 18 U.S.C. § 371. On March 29, 2018, McDonald plead guilty to all counts. U.S. District Court Judge John J. McConnell sentenced McDonald to 39 months incarceration.

- c. **Donald Wicklund** was indicted by a federal grand jury on October 24, 2017, charged with Wire Fraud, 18 U.S.C. § 1343 (2 counts), Fraudulent Use of a Social Security Number, 42 U.S.C. § 408(a)(7)(B) (5 counts), Aggravated Identity Theft, 18 U.S.C. § 1028(A) (5 counts), Bank Fraud 18 U.S.C. § 1344 (3 counts). On April 12, 2018, the Defendant plead guilty to all counts and is currently awaiting sentencing.

19. Wicklund entered into a cooperation agreement with the government. Wicklund engaged in a lengthy interview with investigators. He has testified before the grand jury. During his interview and grand jury testimony, Wicklund implicated Octavio Andres Difo-Castro, who he referred to as “Mono” in a wide-ranging series of frauds including access device fraud, wire fraud, identity theft and conspiracy. Wicklund testified that Difo-Castro was creating false, counterfeit driver’s licenses and recruited people to carry out fraudulent schemes. According to Wicklund, Difo-Castro seldom enters any of the victim business establishments and instead sends individuals he has recruited into the stores to deal with employees. Two of the counts of

the indictment that Wicklund plead guilty to involve the purchase of a silver 2012 Mercedes Benz GLK 350. On or about April 7, 2017, Wicklund purchased a 2012 Mercedes Benz GLK 350 from Elmwood Auto Sales, a Providence used car dealership. He did so by way of a car loan he had fraudulently obtained from the Digital Federal Credit Union. The vehicle identification number for that vehicle is WDCGG8HBOCF749178. According to Wicklund, he had purchased the vehicle for one of his girlfriends. He told investigators that a short time after his girlfriend had taken possession of the vehicle, Difo-Castro took it from her.

20. Wicklund has also told investigators that Difo-Castro was working with a Dominican female he knew as "Pucci." Investigators were able to determine that "Pucci" is Patricia Peralta DOB XX/XX/1991. Agents assembled a series of color photograph of similar looking females and included in the series a photograph of Peralta. Wicklund immediately identified Peralta as the female he knew as "Pucci" who was working with Difo-Castro committing fraud with him. Wicklund claimed that Peralta was involved in credit card fraud at Kohl's Department Store and had fraudulently purchased a Honda motor vehicle.

21. Agents were able to locate a fraudulent transaction carried out by Peralta at Balise Honda in West Warwick, Rhode Island. On or about May 18, 2017, Peralta, using a stolen Social Security Number of XXX-XX-2468, made application for credit to lease a Honda SUV. She listed her employment as Express Wireless in Warwick, Rhode Island. She listed her address as 1 County Street, North Providence, Rhode Island. Agents were able to determine that Peralta was not employed by Express Wireless and she did not reside at 1 County Street, Apartment 11, North Providence, Rhode Island.

22. Agents interviewed the resident of 1 County Street, Frank Arias. Arias was later subpoenaed to appear before the grand jury. He has testified pursuant to a cooperation agreement, that Difo-Castro asked him if he could use his address. Additionally, Arias testified that he worked with Difo-Castro to fraudulently obtain Sprint cellular telephones. Frank Arias testified that Difo-Castro manufactured a counterfeit Rhode Island driver's license using stolen identification information displaying his, Arias's, photograph. Arias has told investigators that he has met "Pucci" and when he first met her she was at Difo-Castro's Pawtucket apartment. According to Arias, "Pucci" was using the computer to buy bitcoin from someone in Colombia. Arias stated that he was aware that "Pucci" and Difo-Castro were involved in fraudulently obtaining loans through the internet. He described a scheme in which "Pucci" and Difo-Castro were creating businesses including business tax ID numbers. Using the business names they then made application through the internet for business loans. Arias was present when Difo-Castro travelled to a Walgreen's Pharmacy to pickup a check that had been sent via commercial carrier to a pickup location at the pharmacy. No payments have been made for the new Honda that Peralta obtained, and its whereabouts are unknown. Arias has testified to buying thousands of dollars worth of fraudulently obtained Apple iPhones from Difo-Castro. Arias has testified he has done so at the behest of the owner of a Metro PCS cellular telephone store located on Warwick Avenue in Warwick, Rhode Island.

23. Further investigation including the review of video surveillance images recorded by Kohl's Department Store's video surveillance cameras revealed that Peralta had committed a series of access device frauds at Kohl's Department Stores located in Massachusetts, Connecticut and Pennsylvania.

24. Difo-Castro has been identified by seven separate witnesses as being an active

identity thief. Four witnesses have provided sworn grand jury testimony that Difo-Castro recruits people to use fraudulent identities to obtain various items including cellular telephones, electronics, furniture and building supplies. These witnesses have further testified that Difo-Castro creates counterfeit identifications and maintains computers and printers for purpose of doing so. The investigation has resulted in the return of an additional indictment charging the following individuals and federal crimes.

- a. Octavio Andres-Difo Castro was indicted by a federal grand jury on July 26, 2018, charged with Conspiracy to Commit Access Device Fraud, 18 U.S.C. § 1029(b)(2), Aggravated Identity Theft, 18 U.S.C. § 1028(A)(1) and (c)(4), Conspiracy to Commit Wire Fraud, 18 U.S.C. 371, Wire Fraud 18 U.S.C. 1343. A warrant was issued for Difo-Castro and on August 9, 2018, he was apprehended in Edgewater, New Jersey.
- b. Patricia A. Peralta was indicted by a federal grand jury on July 26, 2018 and charged as a coconspirator of Difo-Castro. A warrant was issued for Peralta's arrest and on August 9, 2018 she was arrested in Taunton, Massachusetts.

25. Your affiant effected the arrest of Peralta on August 9, 2018. Peralta was in possession of a cellular telephone. I returned Ms. Peralta to the U.S. Secret Service Providence, Resident Office. I provided her with her *Miranda* rights. I audio and video recorded the *Miranda* advisement and the lengthy interview that followed. During my interview, I asked Ms. Peralta about her involvement in various fraud schemes. Ms. Peralta told me that she had worked with Difo-Castro who had enlisted her to participate in a variety of fraudulent schemes including account lookup at Kohl's Department Store, Home Depot and a car loan scheme involving TD Bank. She reported that Difo-Castro had urged her to open TD Bank accounts using the "CPN" he provided her. She was aware that the CPN was a Social Security number

and admitted that she had used this false credit profile to commit other crimes including fraudulently obtaining a Honda SUV. Ms. Peralta told me that she deposited a check from another bank into the TD Bank account and thereafter withdrew money.

26. On August 13, 2018, United States Magistrate Judge Lincoln D. Almond signed a search warrant authorizing the U.S. Secret Service to search Peralta's cellular telephone (18-MJ-253-LDA). I requested Detective Theodore Michaels of the Providence Police to conduct a cellular telephone data extraction. Detective Michaels completed the extraction utilizing accepted practices and software. Detective Michaels has furnished me the reports of that extraction. I have reviewed the images stored on the telephone and I observed that Peralta had been accessing so-called dark web sites in which stolen personal identification information including stolen credit card numbers can be purchased. I have also observed that she has been involved in acquiring and using bitcoin.

27. During the course of the investigation into the fraudulent activities of Martinez, Wicklund and others, agents were in contact with East Providence Police Department Detective Jose Taviera. In July 2018, Detective Taviera provided an East Providence Police report relating to one of a series of fraudulent transactions perpetrated against TD Bank and several credit unions. Your affiant has reviewed the East Providence Police reports as well as a recorded interview of a suspect arrested by the East Providence Police, Jeffry Rodriguez, and have been able to establish the following.

28. On July 28, 2017, members of the East Providence Police Department responded to TD Bank located at 440 Pawtucket Avenue East Providence, Rhode Island. The police had received a report from TD Bank of a male suspect at the bank attempting to carry out a fraudulent transaction. The officers arrived and located a Hispanic male eventually identified as



Jeffry Rodriguez seated in the passenger seat of a 2012 Mercedes Benz GLK 350 with a Vehicle Identification Number of WDCGG8HBOCF749178. When police approached Rodriguez, he identified himself as Juan Ruiz. He was asked for his identification and told the officers that he had left it in the bank. He was asked for his date of birth and hesitated and finally provided a date of birth 11/09/1981.

29. Officers entered the bank and met with Erin Dowlin. Ms. Dowlin was an employee of TD Bank. She turned over a Pennsylvania driver's license bearing the name, Juan Ruiz that displayed a picture of the male the police located in the Mercedes Benz. Ms. Dowlin reported to police that this male was the subject of an internal bank fraud alert. TD Bank security had determined this man had made withdrawals from several accounts held at TD Bank using various names. The source of the funds in those accounts were in part derived from bank checks issued by credit unions for what were later determined to be fraudulent car loans.

30. Police questioned the male and he admitted that his real name was Jeffry Rodriguez and he lives in Providence, Rhode Island. Rodriguez was arrested and found to be in possession of two Pennsylvania driver's licenses bearing his photograph and the stolen identification information of Juan Ruiz and Olban Vega. In addition to the fake driver's licenses, Rodriguez was in possession of a cellular telephone and two counterfeit credit cards one in the name of Olban Vega and one in the name Juan Ruiz.

31. The East Providence Police Department transported Rodriguez to their police station. At the police station, Detective Taviera provided him his *Miranda* warnings. Rodriguez acknowledged he understood his rights and agreed to participate in a video-recorded interview. During the interview, Rodriguez admitted to investigators that he had been hired by a man he

met on the street, who he knew only as "Freddy," to open accounts at TD Bank.<sup>1</sup> He told detectives that after he opened the accounts "Freddy" provided him with bank checks in the names of the accounts he opened. He told investigators that one of the checks was for as much as \$55,000. After he opened the accounts, he deposited the checks and then after a short time he would return to the TD Bank and make withdrawals. He told investigators he would be paid 10% of the amount of the withdrawal. He claimed to be unable to provide any additional information concerning the individual "Freddy" and stated that he had no idea where the checks he deposited came from. Your affiant is aware that at first, Rodriguez told investigators that he was only responsible for making withdrawals from accounts and it was not until detectives had spoken to TD Bank and learned that Rodriguez had actually been responsible for opening accounts and confronted Rodriguez with this information that he admitted to the police he had engaged in that activity as well.

32. The Mercedes Benz GLK 350 with a Vehicle Identification Number of WDCGG8HBOCF749178 that Rodriguez was in is the vehicle that Wicklund purchased with the fraudulent bank loan and which Wicklund claims Difo-Castro took from his girlfriend. When the East Providence Police encountered the vehicle it bore a Rhode Island 20-day temporary plate of 724904. That plate did not belong on the vehicle and is a counterfeit temporary plate.

33. I am aware that a grand jury subpoena was served upon the custodian of records for TD Bank for any documents and records related to the transactions purportedly carried out by Jeffry Rodriguez and which TD Bank had determined were part of the same pattern of activity. I have examined those records and noted that on June 15, 2017, a woman who identified herself as Patricia A. Peralta along with a man who identified himself as Mario G. Lima entered the TD

---

<sup>1</sup> Rodriguez has since told agents that "Freddy" is actually Difo-Castro

Bank in East Providence, Rhode Island and opened joint checking and savings accounts. Peralta provided an address of 1 County Street, Apartment 11 North Providence, Rhode Island and a Social Security number of XXX-XX-2468, this is the same data provided to Balise Honda by Peralta to fraudulently obtain the Honda SUV. One County Street apartment 11 is Frank Arias's address.

34. On June 19, 2017, Peralta deposited a Bethpage Credit Union check in the amount of \$46,000 into the accounts she had opened at TD Bank. She deposited \$45,900 into the checking account and the remaining \$100 into the savings account. The deposit item was a check drawn on the Bethpage Federal Credit Union with the payee identified as Patricia Peralta. On June 22, 2017, a woman who identified herself as Peralta presented herself at the East Providence TD Bank location and withdrew \$9500 in cash from the checking account. On June 29, 2017, a female who identified herself as Peralta appeared at the TD Bank in East Providence and withdrew \$36,460.86. A portion of these funds (\$26,460.86) was in the form of TD Bank official check 31292842-4 payable to Mario G. Lima and \$10,000.00 was in cash. The withdrawal ticket and customer's signature purport to be that of Patricia A. Peralta. On June 30, 2017, official check 31292842-4 was deposited to TD Bank account 8256098259 in the name of Mario G. Lima and Nilka D. Reyes.

35. I have reviewed surveillance images of the individual who opened the Mario G. Lima account and who subsequently made withdrawals from that account. I have positively identified this individual as Angel L. Morales. Morales has a history of arrests for identity theft and is currently wanted in the State of Connecticut for identity theft related charges connected to the bank fraud that is currently the subject of my investigation. Records maintained by the United States Customs and Border Protection show that Angel L. Morales left the United States for the

Dominican Republic on September 3, 2018. This was less than one month after the U.S. Secret Service arrested Octavio Andres Difo-Castro on August 9, 2018, at his Edgewater, New Jersey apartment. Morales left the U.S. after purchasing a one-way ticket to the Dominican Republic.

36. I am aware that a grand jury subpoena was served upon Bethpage Federal Credit Union for records related to the \$46,000 check made payable to Patricia A. Peralta. Bethpage Federal Credit Union has produced records responsive to that subpoena. I have learned that on June 14, 2017, an individual using the personal identification information of Mario Lima, made an online application for a \$46,000 used automobile loan with Bethpage Federal Credit Union. The loan was reportedly for the purchase of a 2015 Ford 150 truck VIN 1FTEW1EG8FFC25174, with the seller identified as Patricia A. Peralta 113 Robinson Street Providence, Rhode Island. Bethpage Federal Credit Union approved the loan and disbursed a \$46,000 check made payable to Patricia A. Peralta. This is the check deposited by Patricia A. Peralta in the account opened at TD Bank.

37. On November 16, 2017, Mario Lima contacted Bethpage Federal Credit Union and reported that he was a victim of identity theft and had never made application for a car loan. Mario Lima provided Bethpage Federal Credit Union with a copy of an East Providence Police report documenting the theft of his personal identification information. I have reviewed East Providence Police report 17-3860-OF and I have learned that on October 25, 2017, Mario Lima and his wife, Patricia Lima responded to the East Providence Police Department to report identity theft. According to Mario Lima, he discovered that someone using his personal identification information had applied for a \$46,000 loan with Pentagon Federal Credit Union. Detective Jose A. Taveira contacted Pentagon Federal Credit Union and learned that the loan had been given to Mario Lima for the private sale of a 2015 Ford F150 Pickup truck. The check was

made payable to the alleged seller of the truck, Nilka D. Reyes, with an address of 1 County Street North Providence, Rhode Island. In support of the loan application, the suspect provided Pentagon Federal Credit Union a copy of a Rhode Island driver's license in the name Mario Lima. The license photo was not that of Mario Lima. The license listed an address of 9 Sullivan Street North Providence, Rhode Island. According to Detective Taveira's report, he was unable to locate 9 Sullivan Street. He was also able to determine that the license number displayed on the license submitted, 9273857 is fraudulent and does not exist. In addition to the copy of the driver's license, the suspect provided Pentagon Federal Credit Union a copy of a title for the Ford F150 truck. The name on the title is Nilka D. Reyes 1 County Street Apartment 10 North Providence, Rhode Island. The VIN for the truck is listed as 1FTEW1EG8FFC25174, the same number submitted to Bethpage Federal Credit Union to secure a loan from them in the form of a check payable to Patricia A. Peralta. Patricia A. Peralta has previously used the address of 1 County Street North Providence, Rhode Island as her address.

38. Through my examination of the records supplied by TD Bank, I have learned that on June 30, 2017, a man representing himself to be Mario G. Lima with an address of 18 Henry Street Providence, Rhode Island opened TD Bank checking and savings accounts at the Pawtucket Branch of TD Bank. On July 9, 2017, a female, representing herself to be Nilka D. Reyes with the same address of 18 Henry Street, was added as a joint account holder with Lima. On July 10, 2017, the male deposited the above referenced \$46,000 check from Pentagon Credit Union payable to Nilka D. Ryes and Mario Lima. This check corresponds to the check issued by Pentagon for the alleged sale of the Ford F150 pickup truck. The proceeds of that deposit were withdrawn in \$9500 increments over the course of 8 days. As referenced above, the individual involved in opening the Mario G. Lima accounts is Angel L. Morales. Postal Inspectors located

the Nilka Reyes whose identification was used to add her as a signatory to the TD Bank account. Nilka Reyes resides in Puerto Rico and denied any involvement in opening the account in question.

39. At the time of his arrest by the East Providence Police Department, Jeffry Rodriguez was in possession of counterfeit Pennsylvania drivers' licenses in the name Juan O. Ruiz and Olban P. Vega.

40. Records produced by TD Bank and the Alliant Credit Union, responsive to grand jury subpoenas document that on or about July 17, 2017, the Alliant Credit Union issued a check payable to Juan Ruiz in the amount of \$55,000. The check was presumably for the purchase of a 2015 Chevrolet Corvette VIN 1G1YK2D77F5124612 with Juan O. Ruiz purportedly selling the vehicle to Robert Rocchio. The check was generated by Alliant representing an automobile loan to someone representing themselves to be Robert Rocchio. According to Alliant's records, someone made application with Alliant for an online car loan using the personal identification information of Robert Rocchio. No payments were made on the loan. Alliant conducted an investigation and determined that Robert Rocchio's identification had been stolen and used to open accounts and apply for a loan. Alliant Credit Union produced a copy of the Rhode Island driver's license submitted to them as proof of identity. The license number 5497786 is not on file with the Rhode Island Registry of Motor Vehicles and was counterfeit.

41. A review of records produced by TD Bank responsive to the grand jury subpoena reveals that on July 7, 2017, an individual now known to be Jeffry Rodriguez, opened a checking and savings account with TD Bank at their Rumford, Rhode Island location in the name Juan Ruiz. On July 17, 2017, Alliant Credit Union issued a check in the amount of \$55,000 payable

to Juan Ruiz. In the memo section of the check is the name Robert Rocchio with a vehicle identification number. On July 18, 2017, Jeffry Rodriguez deposited the check payable to Juan Ruiz into the TD Bank checking account he had opened in that name. On July 19, 2017, he made a \$9300 cash withdrawal. On July 21, 2017, he made a \$9400 cash withdrawal and on July 24, 2017, he made an \$8900 cash withdrawal.

42. A review of records produced by TD Bank responsive to a grand jury subpoena reveals that on July 12, 2017 an individual now known to be Jeffry Rodriguez made application with TD Bank at their North Attleboro, Massachusetts branch for checking and savings accounts in the name of Olban Vega. Vega (Rodriguez) presented a Pennsylvania driver's license in the name Olban Vega as proof of identification. Bethpage Federal Credit Union had issued a check for \$55,000 made payable to Olban Vega on July 11, 2017. In the memo portion of the check is the name Robert Rocchio. On July 13, 2017, Vega (Rodriguez) deposited the \$55,000 check into the checking account. On July 14, 2017, he withdrew \$9500 in cash from the North Attleboro, Massachusetts branch of TD Bank. On July 22, 2017, he withdrew \$9000 from the Johnston, Rhode Island branch of TD Bank. On July 25, 2017 he withdrew \$9100 in cash from the Johnston, Rhode Island branch of TD Bank. On July 27, 2017, TD Bank discovered the check had been issued by Bethpage based upon a fraudulent loan application and the funds were subsequently frozen.

43. On August 9, 2018, United States Secret Service agents arrested Octavio Andres Difo-Castro at an Edgewater, New Jersey apartment he had rented using a stolen identity. Difo-Castro was taken into custody and a federal search warrant was obtained for his apartment. United States Magistrate Judge Mark Falk, District of New Jersey, issued a search warrant for apartment 312, 100 Alexander Way Edgewater, New Jersey (18-MJ-3675). During the course of

the search, Secret Service agents discovered several identity theft packages. These packages, which were labeled with the name of the identity theft victim and contained a written list of the fraudulent documents contained in the Manilla envelope, included counterfeit Social Security cards and counterfeit Pennsylvania driver's licenses. In addition to the packages, agents discovered a spiral notebook replete with references of stolen identification information and notations relating to ongoing bank frauds. Numerous documents seized have been tied to reported instances of bank fraud.

44. In addition to the documentary evidence briefly described above, agents located numerous electronic devices (TARGET DEVICES) including ten cellular telephones, an Apple Macbook Pro 15" computer, Apple iMac 27" desktop computer, and external computing devices (a USB flash drive, SD cards). Those devices, seized from the apartment are described more fully below:

- a) Motorola Moto phone (Gold in color) – IMEI – 355674083917180
- b) Toshiba USB flashdrive (white in color) – S/N – 134013XA475CARGO1S
- c) Samsung phone (grey in color, model SM-J327T1) – IMEI – 354256/09/752960/6
- d) Coolpad phone (black in color) – IMEI – 862429030253312
- e) LG phone (grey in color, model LM-X210MA) – IMEI – 356233-09-257593-2
- f) 16GB SanDisk SD Card - BL1418250167G
- g) 16GB SanDisk SD Card – BL1731250835G
- h) LG (grey in color, model LM-X210MA) – IMEI – 356233-09-258022-1
- i) Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091035663
- j) Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091522652
- k) iPhone X (silver in color) a label with the #13 has been affixed to the phone
- l) iPhone X (space grey in color) a label with the #14 has been affixed to the phone
- m) LG phone (black in color, model LM-X210MA) – IMEI – 357093-09-047884-7
- n) LG phone (grey in color, model LM-X210MA) – IMEI – 356233-09-664656-4
- o) 64GB SD card in Canon SanDisk – BN1734951494G
- p) Apple Macbook Pro 15" (MODEL A1707) S/N – C02VW0DYHTD6
- q) Apple iMac 27" - S/N – C02VW37VHX87



45. I have examined Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091522652. On the back of the phone is a typewritten sticker in the name Kevin G. Phillips. The sticker contains a Social Security number and date of birth and address. Through my investigation, I have determined that the name and personal identification information of Kevin G. Phillips was used in June of 2018 to apply for an automobile loan with the Alliant Credit Union. That loan application was determined by the credit union to be fraudulent and was denied.

46. I have also examined Motorola Moto phone (gold in color, model XT1765) – IMEI – 354135091035663. On the back of the phone is a typewritten sticker in the name Sergio A. Aragao, an address, Social Security Number and date of birth. In Difo-Castro's apartment, agents located a Digital Federal Credit Union "Intent to Sell Form" listing the buyer as Sergio A. Aragao. With that form as a print-out containing detailed personal identification information of Sergio A. Aragao. A grand jury subpoena has been served upon Digital Federal Credit Union seeking documents relating to the Aragao transaction.

47. Based upon my experience and training it is apparent to me that Difo-Castro was labeling various cellular telephones with the personal identification information of his identity theft victims. In this way, Difo-Castro was able to associate a particular cellular telephone number with a particular fraudulent scheme and would know when a call or text was coming in on a particular device which fraudulent scheme was involved. This evidence further establishes the probable cause to believe that relevant and material evidence will be found on these devices.

48. On August 15, 2018, Jeffry Rodriguez was arrested pursuant to a federal arrest warrant and complaint signed by United States Magistrate Judge Lincoln D. Almond. Jeffry Rodriguez was charged by the United States Attorney on September 12, 2018 by way of a

Criminal Information that alleged Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349, Bank Fraud 18 U.S.C. § 1344(2), and Aggravated Identity Theft, 18 U.S.C. § 1028(A)(a)(1). On September 20, 2018, the Defendant plead guilty to all counts and is currently awaiting sentencing.

49. As part of his plea agreement, Jeffry Rodriguez has agreed to cooperate with the United States in its ongoing investigation into the criminal activities of Octavio Andres Difo-Castro and others.

50. On August 29, 2018, Jeffry Rodriguez, with the assistance of his attorney, Joseph Voccola, participated in a lengthy proffer interview. During the course of this proffer interview, Jeffry Rodriguez explained that he had become involved in the above described bank fraud scheme at the request of a man he knew as “Mono.” He also knew “Mono” as Andres. Agents showed him a photographic array of six color photographs one of which was a known photograph of Difo-Castro. Jeffry Rodriguez immediately selected the photograph of Difo-Castro as being the person he knew as “Mono” or Andres. According to Rodriguez, Difo-Castro has been working with Angel Morales, Patricia Peralta and Rolondo Estrella in creating bank accounts using stolen identification information.<sup>2</sup> According to Rodriguez, Difo-Castro recruited him to enter various banks and open accounts in the names of identity theft victims. He reported that Difo-Castro provided him with counterfeit Pennsylvania driver’s licenses to use to open the accounts. He further stated that he opened the accounts for the purpose of depositing checks derived from fraudulently obtained car loans. Rodriguez explained that he had also been involved with Difo-Castro in fraudulently obtaining cellular telephones using counterfeit

---

<sup>2</sup> Rodriguez did not know the full identity of Peralta or Estrella. He knew Peralta as Pucci and Estrella as Rolondo. He selected a photograph of Peralta from a photo array and identified her as Pucci. He was shown a photographic array containing a photograph of Rolondo Estrella and identified that photograph as the person he knew as Rolondo.

government identification. Rodriguez has stated that he continued to be involved in working with Difo-Castro in the bank fraud scheme after his arrest in East Providence. As recently as August of 2018, he travelled to Key Bank in Connecticut for purposes of depositing a fraudulently obtained car loan check.

51. Through my experience and training coupled with the facts I have uncovered during the course of this investigation, I know that Octavio Andres Difo-Castro has repeatedly used Google email accounts to perpetrate his fraudulent schemes. As is set out more fully below, my investigation in this case has uncovered evidence documenting Difo-Castro's use of email accounts and electronic devices to carry out his fraudulent schemes.

52. On September 7, 2017, United States Magistrate Judge Lincoln D. Almond, signed a search warrant directed to Google for content of Google email account money7877@gmail.com (17-MJ-406 A). I served that warrant on Google and received an extensive amount of email data including attachments. I reviewed this data and noted that the account was used extensively to exchange stolen personal identification information as well as photographs of accomplices to attach to counterfeit government identifications. I have interviewed Donald Wicklund concerning this account. Wicklund has admitted to having used this account but stresses that Octavio Andres Difo-Castro had complete access to the account. Wicklund has further stated that certain emails including one containing an attachment used to create counterfeit identifications was definitely sent by Difo-Castro.

53. On January 29, 2018, United States Magistrate Judge Patricia A. Sullivan, issued a search warrant for a Samsung cellular telephone Model SM-G550T1 (18-MJ-29-PAS). This cellular telephone was seized incident to the arrest of Jason McDonald. A data extraction of that

cellular telephone evidenced the fact that members of the conspiracy engaged in an extensive amount of identity theft related email correspondence.

54. Additionally, I am aware that Jeffry Rodriguez and Patricia Peralta are members of a criminal conspiracy creating online banking accounts utilizing stolen personal identification. These accounts are in the name of individuals the group claims are sellers of motor vehicles. The conspirators also open accounts using stolen personal identification information for the purported buyers of the car. The buyers then make application for automobile loans to purchase vehicles from the sellers. The victim financial institutions approve the loans and disburse checks in the name of the sellers of the cars. Those checks are then deposited into the sellers account and are then withdrawn in cash or transferred over to other accounts for eventual withdrawal. I am aware that such an operation requires up to the minute coordination such as would be facilitated by the use of cellular telephones like the devices seized by the Secret Service from Difo-Castro's Edgewater, New Jersey apartment. I am also aware, as was borne out through the examinations of Reynaldo Martinez's and Jason McDonald's cellular telephones, that identity thieves will use the SMS and email features of their cellular telephones to exchange and store the stolen personal identification of their victims. I am also aware as was established through the examination of Patricia Peralta's cellular telephone, that these individuals will often take photographs or "screen shots" of identification documents they intend to use to carry out fraud. I am also aware that runners in an operation like this one will often electronically transmit photographs of themselves to the manufacturer of the counterfeit identifications and will do so by attaching the photographs to SMS messages or emails. I am aware that during his interview with the East Providence Police Jeffry Rodriguez told the investigators that he had a photo taken of himself at a Walgreens and had done so for the express purpose of having it affixed to a

counterfeit driver's license. A compact disc containing an electronic photograph of Jeffry Rodriguez bearing the label of Walgreens was seized from Difo-Castro's Central Avenue Pawtucket, Rhode Island apartment. Additionally, in a situation such as that in which Rodriguez was involved, runners will receive instructions and directions through their cellular telephones.

55. The investigative team has determined that as part of the scheme a large number of cell phones had been purchased at various cell phone stores throughout Rhode Island and Massachusetts using false identities. During his post arrest, recorded interview, Donald Wicklund admitted to having fraudulently obtained over one hundred cellular telephones. Wicklund worked with Martinez and others to obtain the phones and then sell them to a Warwick, Rhode Island cellular telephone store. In furtherance of this investigation, the investigative team contacted Sprint Corporate Security to notify them of the fraud. Additionally, Sprint was served with several grand jury subpoenas seeking certain transaction records and video surveillance footage. One subpoena requested data related to the purchase of cellular telephones from the Cranston, Rhode Island Sprint Store using the name, Charles McCain.

56. Sprint produced records responsive to the subpoenas including the sales records related to the McCain transaction. Sprint has reported that in the ordinary course of their business they will electronically scan a copy of the photo identification presented by the customer opening the account. Sprint captures identification numbers appearing on both the front and back of the identification. Additionally, Sprint will often request the customer provide an email address and alternate telephone numbers. Sprint representatives have told me that when they began to look into the data related to the McCain Cranston, Rhode Island transaction, they were able to identify a series of linked fraudulent transactions. Sprint linked the transactions by establishing that the perpetrators used reoccurring driver's license numbers (either from the front

or the back of the license and common email addresses). Using these links, Sprint was able to show that several of the fraudulent accounts utilized an email address of

Onlineworkperfect@gmail.com

57. During my interview with Wicklund on February 7, 2018, he told me that an individual he knows as "Mono" primarily used the email address onlineworkperfect@gmail.com.

Wicklund has testified under oath that "Mono" is Octavio Andres Difo-Castro.

onlineworkperfect@gmail.com is the same email address that Sprint has linked to numerous fraudulent accounts. Wicklund claims that Mono uses onlineworkperfect@gmail.com to carry out identity fraud related schemes. Wicklund claimed that Difo-Castro is a prolific fraudster who uses runners he recruits from Mexico and the Dominican Republic to use counterfeit identification created with stolen personal information to obtain various goods including building supplies, electronics, and cellular telephones. Wicklund claims to have worked in concert with Difo-Castro in committing identity theft. I am aware that Wicklund selected a photograph of Difo-Castro from an array of men of similar appearance and identified the individual depicted known variously as Mono, Andres, Difo-Castro.

58. On February 26, 2018, your affiant obtained a search warrant for the above listed Gmail account, onlineworkperfect@gmail.com. After reviewing the account, your affiant located an additional Google account identified as turealnegrubello247@gmail.com. Numerous emails containing Personally Identifying Information were forwarded from onlineworkperfect@gmail.com. Seventy-one emails were forwarded to turealnegrubello247@gmail.com from onlineworkperfect@gmail.com. Many of the emails contain images depicting individuals your affiant believes were having fake identification cards made. An email sent on February 10, 2017, contains an image of Patricia Peralta. During the

above described interview with Peralta on August 9, 2018, she stated that Difo-Castro would provide her with an ID with her photo. Your affiant has also located several counterfeit Identifications through the course of this investigation with the exact image from the email.

59. An email sent from [onlineworkperfect@gmail.com](mailto:onlineworkperfect@gmail.com) to the target account on May 28, 2017, contains a link to the 2016 American Association of Motor Vehicle Administrators DL/ID Card Design Standard. This PDF Document is the standard used by North America to create their State identification cards. It provides specific standards used in North America. Your affiant believes that Andres Difo-Castro utilized this information to assist him in creating high quality, up to North American Standard, fake Identification cards.

60. In an email dated December 18, 2016, a Photoshop file titled: ENDA CURRID.psd is attached being sent from [onlineworkperfect@gmail.com](mailto:onlineworkperfect@gmail.com) to the target email address, [turalnegrobello247@gmail.com](mailto:turalnegrobello247@gmail.com). Your affiant opened the attached file using Photoshop and observed that the file contained a template to make a Rhode Island Drivers License. The file also contained numerous individuals' photographs that were saved into the file. The same file was also located in an additional location on an email account belonging to Donald Wicklund, an indicted coconspirator.

61. Gmail contacts located in [Onlineworkperfect@gmail.com](mailto:Onlineworkperfect@gmail.com) include many email addresses linked to other frauds such as: [lblanco221@gmail.com](mailto:lblanco221@gmail.com) (Lardyn Blanco co-operating witness), [moneym7877@gmail.com](mailto:moneym7877@gmail.com) (Wicklund indicted co-conspirator), [pachi2203@hotmail.com](mailto:pachi2203@hotmail.com) (Patricia Peralta indicted coconspirator), [gracebella24@gmail.com](mailto:gracebella24@gmail.com) (Grecia Bello Cooperating witness), [turalnegrobello247@gmail.com](mailto:turalnegrobello247@gmail.com) (Andres Difo listed as name on account according to Gmail).

62. During my interview of Reynaldo Martinez after his arrest on May 24, 2017,

Martinez identified Andres Difo-Castro as the guy in charge. Martinez said that he used the email account [turealnegrubello247@gmail.com](mailto:turealnegrubello247@gmail.com) to send information.

63. In an email dated March 19, 2017, a photo of Frank Arias, a cooperating witness, is attached being sent from [Onlineworkperfect@gmail.com](mailto:Onlineworkperfect@gmail.com) to [turealnegrubello247@gmail.com](mailto:turealnegrubello247@gmail.com). The photo is similar to those used to make fake Identifications.

64. In an email dated March 25, 2017, a photo of Israel Vellasco, aka "The Mexican", is attached to an email from [Onlineworkperfect@gmail.com](mailto:Onlineworkperfect@gmail.com) to [turealnegrubello247@gmail.com](mailto:turealnegrubello247@gmail.com). The photo is similar to those used to make fake Identifications. On May 9, 2017, Israel Vellasco was arrested by the Mansfield, Massachusetts police department attempting to obtain cellular telephones using fraudulent identification. He was arraigned on identity theft related charges. He failed to appear for his pretrial conference and is currently wanted. Vellasco's photograph was affixed to at least five counterfeit driver's licenses used to fraudulently obtain iPhones from Sprint. Vellasco was also Difo-Castro's roommate while Difo-Castro resided in a loft apartment at the Westfield Lofts in Providence, Rhode Island.

65. In an email dated April 8, 2017, sent from [Onlineworkperfect@gmail.com](mailto:Onlineworkperfect@gmail.com) to [turealnegrubello247@gmail.com](mailto:turealnegrubello247@gmail.com) a photo of Jeffry Rodriguez was attached. The photo is similar to those used to make fake Identifications.

66. In an email dated June 13, 2017, sent from [Onlineworkperfect@gmail.com](mailto:Onlineworkperfect@gmail.com) to [turealnegrubello247@gmail.com](mailto:turealnegrubello247@gmail.com) a photo of Patricia Peralta's legitimate Driver's license was attached.

67. This extensive investigation focusing on Martinez, Wicklund, McDonald, Peralta and Difo-Castro (among others) has revealed that these individuals have committed identity fraud in a coordinated fashion. They have provided support to each other in carrying out their fraudulent

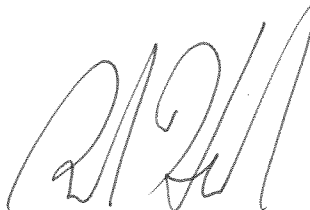


schemes and have routinely relied upon the electronic transfer of information and data through email and text messaging to carry out their offenses. The investigative team has determined that the TARGET ACCOUNT has been utilized by Difo-Castro to commit identity fraud and related federal offenses. Additionally this individual along with other coconspirators have used email as a way to transmit photographs and other information relating to their criminal activity.

68. The evidence uncovered has demonstrated that Difo-Castro relies heavily upon electronic communication devices to send and receive communications vital to the success of his fraudulent schemes. Moreover, Difo-Castro extensively uses computing devices to obtain stolen personal identification information, fraudulently open bank accounts and apply for fraudulent bank loans. Additionally, the scope of Difo-Castro's fraudulent scheme is so broad it is necessary for him to keep records to keep track of loans he has applied for, the names and personal information he has provided to lending institutions, the names of the institutions where he has opened accounts to deposit fraudulently obtained loans and the amounts received. Difo-Castro has relied in part of written notations to track such information however, the amount of records seized from his apartment although extensive do not represent the true scope of the fraudulent schemes he has perpetrated. It is therefore likely that additional records will be found on the computing devices seized from his apartment.

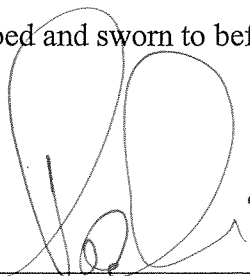
69. Based on the information described above, I have probable cause to believe that The TARGET DEVICES, contain evidence of violations of federal law including, Conspiracy to commit Aggravated Identity Theft, 18 U.S.C. § 1029(b)(2); Identity Theft, 18 U.S.C. § 1028A, Access Device Fraud, 18 U.S.C. §1029, Bank Fraud 18 U.S.C. § 1344 and Fraudulent Use of Social Security Numbers 42 U.S.C. § 408(a)(7)(B) as described more fully in Attachment A.

I declare that the foregoing is true and correct.

A handwritten signature in black ink, appearing to read 'B. Henderson', written over a horizontal line.

Brandon Henderson  
Special Agent  
U.S. Secret Service

Subscribed and sworn to before me this 26<sup>th</sup> day of September, 2018.

A handwritten signature in black ink, appearing to read 'Patricia A. Sullivan', written over a horizontal line.

HONORABLE PATRICIA A. SULLIVAN  
UNITED STATES MAGISTRATE JUDGE  
DISTRICT OF RHODE ISLAND

## ATTACHMENT A

1. All records on the TARGET DEVICES that relate to violations of federal law including Conspiracy to commit Aggravated Identity Theft, 18 U.S.C. § 1029(b)(2); Identity Theft, 18 U.S.C. § 1028A, Access Device Fraud, 18 U.S.C. § 1029, Bank Fraud 18 U.S.C. § 1344 and Fraudulent Use of Social Security Numbers 42 U.S.C. § 408(a)(7)(B) and involve Octavio Andres Difo-Castro, Angel L. Morales, Patricia A. Peralta and others since January 1, 2016, including:

- a. Lists of personal identification information of identity theft victims to include their name, date of birth, Social Security Number, address, employment and mother's maiden name; lists of customers and related identifying information;
- b. Bank account numbers and the names associated with the accounts, copies of checks issued by lending institutions, correspondence received from banks and credit unions, loan applications, copies of motor vehicle titles and bills of sale
- c. Any information related to the disposition of the illegally obtained funds including records of wire transfers, Moneygram and Western Union documentation evidencing the movement of money both within and outside of the United States;
- d. Copies of counterfeit government identification documents to include any templates used in the creation or reproduction of such documents;

- e. All bank records, checks, credit card bills, account information, and other financial records.
  - f. Any screen shots of internet websites displaying personal identification information to include credit card numbers;
  - g. Any information documenting how to carry out identity theft related schemes including visits to any internet websites such as YouTube;
  - h. Photographs of coconspirators as well as photographs to be used to create counterfeit government identifications;
  - i. Records documenting the purchase of items including motor vehicles;
  - j. Records documenting the shipment of goods outside of the United States
2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Records evidencing the use of the Internet to communicate with Gmail accounts, financial institutions, vendors of holograms used to authenticate government identifications to include:
- a. records of Internet Protocol addresses used;
  - b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.